ESET®

THREAT HUNTING

On-demand threat investigation, root cause analysis and remediation advice without the need for extra internal resources

ESET® ENJOY SAFER TECHNOLOGY™

30 30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ESET Threat Hunting service helps customers investigate a certain set of data, events and alarms generated by ESET's endpoint detection and response solution—ESET Enterprise Inspector.

Why ESET Threat Hunting service?

GET THE MOST OUT OF ESET'S EDR

ESET Enterprise Inspector is a sophisticated EDR tool for identification of anomalous behavior and breaches, risk assessment, incident response, investigation and remediation.

It monitors and evaluates all activities happening in the network in real time and allows organizations to take immediate action if needed.

ESET Enterprise Inspector is a prerequisite for ESET Threat Hunting service.

LACK OF PRODUCT KNOWLEDGE

Utilizing new products without any previous knowledge can become tricky even for organizations with dedicated security or IT teams. In addition, keeping up with the rapidly changing cyber threat landscape can be challenging and sometimes best left to experts.

LACK OF MANPOWER

Helps security teams and IT administrators prioritize their workload by pinpointing only the important events. In addition, an organization can take months to hire and train a team to implement and monitor an Endpoint detection and response platform.

REST EASY

If any anomalies or breaches are identified, our experts can quickly find the root cause and remediate the issues that were found for good.

LONG-TERM COSTS

Creating dedicated teams and/or hiring specialists to perform niche occasional tasks can incur high long-term costs. Purchasing products and services from a single vendor reduces complexity for accounting departments—especially for multinational corporations that would otherwise be left with a large number of regional providers.

ESET Threat Hunting service technical features

ON-DEMAND

Organizations contact ESET Threat Hunting operators when they require Threat Hunting services.

ROOT CAUSE ANALYSIS

Threat Hunting operators review highlighted alarms to determine their root cause.

ACTIONABLE ADVICE

Operators review alarms and compile their findings into a comprehensible status report as well as provide actionable advice to the organization.

SUBSCRIPTION BASED

Organizations purchase Threat Hunting services in customizable time blocks during which ESET experts are ready to investigate threats when most needed.

ON-PREMISE DATA

All threat and organization data continue to stay on-premise by setting up a secure VPN connection between ESET and the organization.

INITIAL ASSESSMENT

A thorough initial assessment is completed to assess the specific organizations security policies as well as develop an internal profile.

The stages

Initial assessment

- Each service starts with an assessment of not just the customer's environment but organizational composition and general cybersecurity attitude.

- A full interview is completed with relevant organizational staff members to collect all required information.

- The result of this phase is an Organization Security Profile which can be consulted in the future by any Threat Hunting operator that requires specifics related to the organization to make correct judgments.

- Organizations are recommended to contact ESET with any changes to their environment due to the on-demand nature of the Threat Hunting service.

Regular operation

- When requested, ESET Security experts begin the investigation of pinpointed events to determine their root cause and provide actionable advice customized to the specific organization.

- Findings from each investigation are compiled into comprehensible status reports that express technical details in human-readable language.

ESET IN NUMBERS

110m+
users worldwide

400k+
business customers

200+
countries & territories

13
global R&D centers